REMARKS/ARGUMENTS

Favorable reconsideration of this application as presently amended and in light of the following discussion is respectfully requested.

Claims 1, 2 and 4-19 are pending in the present application. Claim 3 has been canceled and Claims 1, 2, 5, 11, 17 and 19 have been amended by the present amendment.

In the outstanding Office Action, Claims 1, 5-11, 14-16 and 19 were rejected under 35 U.S.C. § 102(b) as anticipated by Adams, Jr. et al.; Claims 2-4 were rejected under 35 U.S.C. § 103(a) as unpatentable over Adams, Jr. et al.; Claims 12 and 13 were rejected under 35 U.S.C. § 103(a) as unpatentable over Adams, Jr. et al. in view of Perlman; and Claims 17 and 18 were rejected under 35 U.S.C. § 103(a) as unpatentable over Adams, Jr. et al. in view of Saito.

The present invention is directed to a relay device in which the contents protection information is information necessary to perform a contents protection procedure including at least an authentication and/or a key exchange between one device/service/sub-unit on the first network and another device/service/sub-unit on the second network, or the relay device that performs the contents protection procedure including at least an authentication and/or a key exchange, separately with respect to one device/service/sub-unit on the first network and with respect to another device/service/sub-unit on the second network.

On the contrary, Adams, Jr. et al. discloses an encryption/decryption device, which is to be spliced in the local area network, and which selectively encrypts or decrypts only the data portion of a data packet, leaving the routing information contained in the header and trailer portions of the data packet unchanged (see the abstract). The present invention is not directed to such an encryption/decryption device that selectively encrypts/decrypts only the data portion, without encrypting/decrypting the routing information in the header.

That is, Adams, Jr. et al. does not teach or suggest a contents protection procedure including at least an authentication and/or a key exchange. The outstanding Office Action interprets the contents protection procedure as being the same as encryption/decryption, but the authentication and/or key exchange are procedures to be performed between two nodes that wish to communicate with each other, for authenticating each other or sharing a key to be used for encryption/decryption. These procedures do not encrypt/decrypt anything, so that they are different from the encryption/decryption process.

In more detail, the outstanding Office Action indicates Adams, Jr. et al. discloses the claimed features in columns 4, lines 40-52; column 5, lines 2-5; column 5, line 61 to column 6, line 5; column 6, lines 6-16 and 21-29; and column 6, line 65 to column 7, line 11.

However, Applicants note column 4, lines 40-52 only discloses a table to be used in making a routing or encryption/decryption decision, which includes keys for encrypting and decrypting data. This portion of Adams, Jr. et al. does not mention anything about authentication or key exchange. In addition, column 5, lines 2-5 only mentions the upstream port and the downstream port. Further, column 5, line 61 to column 6, line 5 only discloses that the header includes a source and destination, checksums and option bits such as that which indicates that the data are encrypted. Likewise, column 6, lines 6-16 only discloses the extraction of the header information and the comparison of the extracted header information with a key list at a time of the encryption. Further, column 6, lines 21-29 only discloses that the key list contains keys for encrypting/decrypting data and handling information. Column 6, line 65 to column 7, line 11 only discloses the reconstruction of the IP data packet using the encrypted data. The above-noted portions noted do not teach or suggest anything about authentication or key exchange.

Thus, Adams, Jr. et al. does not teach or suggest the claimed contents protection procedure including at least an authentication and/or a key exchange nor the claimed contents

protection information reception unit and the contents protection information transfer unit of Claims 1 and 2, the first contents protection unit and the second contents protection unit of Claims 5, 11 and 19, the copy protection processing unit of Claims 12, 13, 14 and 16, and the first copy protection processing unit and the second copy protection processing unit of Claim 17. Saito also does not teach or suggest the claimed invention.

Further, regarding Claims 12 and 13, the outstanding Office Action recognizes that Adams, Jr. et al. fails to disclose the features regarding the authentication target query and reply, and relies on Perlman as teaching thee features and cites col. 14, lines 38-49. However, this section only describes the query from the network manager to each node to determine if it received a particular packet. This portion of Perlman does not disclose a query and reply regarding a service/sub-unit/plug that is transferring the encrypted contents, to ascertain which service/sub-unit/plug is transferring the encrypted contents.

Accordingly, it is respectfully submitted independent Claims 1, 2, 5, 11-14, 16, 17 and 19, and each of the claims depending therefrom are allowable.

Consequently, in light of the above discussion and in view of the present amendment, the present application is believed to be in condition for allowance and an early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870
David A. Bilodeau
Registration No. 42,325

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/03)

I:\ATTY\DAB\00397378-AM.DOC